

MULTIMEDIA



UNIVERSITY

STUDENT ID NO

--	--	--	--	--	--	--	--	--	--

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 1, 2016/2017

TAC3121 – APPLIED CRYPTOGRAPHY (All Sections / Groups)

11th OCTOBER 2016
9.00 a.m – 11.00 a.m
(2 Hours)

INSTRUCTIONS TO STUDENT

1. This Question paper consists of 3 pages with 5 Questions only.
2. Attempt **ALL** questions. All questions carry equal marks (10) and the distribution of the marks for each question is given.
3. Please print all your answers in the Answer Booklet provided.

Question 1

- 1a) State if it is possible to use a hash function to construct a block cipher with a structure similar to DES because a hash function is one way and a block cipher must be reversible. (3)
- 1b) Describe why there is a need for public-key certificate and explain the process involved in certificate creation? (3)
- 1c) State the difference between differential and linear cryptanalysis. (2)
- 1d) State the difference between diffusion and confusion. (2)

Question 2

- 2a) Explain a digital signature and how is it used in the public-key certification. (3)
- 2b) Explain why is the middle portion of triple DES a decryption rather than an encryption. (2)
- 2c) Explain the purpose of S-boxes in Data Encryption Standard (DES). (1)
- 2d) Explain how **confidentiality** and **message integrity** are implemented in respect to cryptography. (2+2)

Question 3

- 3a) Users A and B use the Diffie Hellman key exchange technique with a common prime $q = 71$ and a primitive root $\alpha = 7$.
 - i) If user A has private key $X_A = 5$, compute A's public key Y_A . (1)
 - ii) If user B has private key $X_B = 12$, compute B's public key Y_B . (1)
 - iii) Determine the shared secret key? (2)
- 3b) Determine the RSA private key given the parameters below. (3)

 $p = 11, q = 3, e = 3$
- 3c) Explain how hash function is used to create digital signatures with the help of a diagram. (3)

Continued...

Question 4

- 4a) Describe TWO disadvantages of Symmetric-Key Cryptography. (2)
- 4b) Explain the security advantage of Elliptic Curve Cryptography. (2)
- 4c) Explain and give usage example (each) for Electronic Codebook Book (ECB) and Cipher Block Chaining (CBC). (4)
- 4d) Describe ONE advantage and ONE disadvantage of using Counter (CTR). (2)

Question 5

- 5a) Compute the multiplicative inverse of each nonzero element in Z_5 . (2)
- 5b) For group S_n of all permutations of n distinct symbols, (2)
 - i) Compute the number of elements in S_n ?
 - ii) Show that S_n is not abelian for $n > 2$.
- 5c) Using Fermat Theorem, compute $3^{201} \bmod 11$. (2)
- 5d) Compute $\gcd(24140, 16762)$. (4)

End of Page